Hacking cyber-risks back in their tracks: to identify the right supply chain controls, look at the system

Sepúlveda, Daniel; Khan, Omera

Published in:
Effektivitet

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

effektivitet » dk

Hacking cyber-risks back in their tracks: to identify the right supply chain controls, look at the system

A more comprehensive way of looking at cyber-risks in supply chains is required, when considering the increasing complexity of the supply networks and the exposure to unexpected disruptions, caused by cyber-attacks. This article describes some of the reasons why current risk assessment methods are insufficient. The article provides an analogy for understanding the dynamic effects in a company. It describes in general terms what it means to understand cyber-risks from the control perspective, and it describes a new way to understand supply chain resilience. The focus is changed from the reliability of the supply chain components to the control and a deeper understanding of the supply chain system.

Af Daniel Sepúlveda, MSc., PhD researcher, DTU Management Engineering, dasep@dtu.dk

We are creating a complex world

The complex supply chains we continue to build, are creating many new vulnerabilities, exposing organizations to new risks. Many of these risks originate from the increasing dependence on information technology (IT) by competitive supply chains. Organizations are damaged by disruption of operations, and loss of company data, intellectual property and organizational value. Studies have showed costs at over 550 billion USD annually1. These disruptions are challenging the way we organize our operational activities, as well as the way we manage the relationships with our partners. It also signifies that the transparent and rapid access to company resources enabled by IT in the supply chain, is also a platform used by intruders for their own benefit.

The diversity of potential disruptions is making traditional risks assessment tools impractical. Companies do not have the resources to analyze every potential failure, and to update the assessments as new risks appear, or existing risks change.

Our research at the Technical University of Denmark (DTU) is leading us to challenge the traditional risk analysis used in complex supply chains. I Improvements can be achieved by going from a static analysis, based on analyzing reliability of components, to a dynamic analysis, based on control of vulnerabilities in the organization.

In a previous article in this magazine (see "The rising threat of cyber risks in supply chains"), Prof. Omera Khan from the Technical University of Denmark analyzed the threat of these attacks. That article outlined the forms these attacks are taking and some of their impacts, and it outlined steps for building cyber-resilience into the supply chain. This article goes a step further by proposing to look at cyber-risks with a systemic perspective. Although this novel approach requires a change in the way these risks are understood, it can create a comprehensive way of understanding the supply chain structure, for improving supply chain reaction and recovery (resilience) when an unexpected cyber-attack occurs.

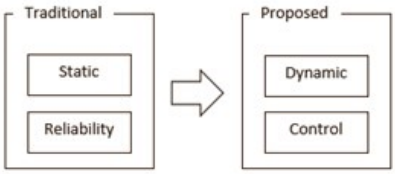

Figure 1 Proposed risk analysis change

Current approaches to cyber-risk have shortcomings

The Federal aviation administration in the US recently identified more than one hundred methods for assessing risks2 several of which are traditionally used in supply chains. These methods are largely based on the assumption that an undesirable event is caused by a chain of other preceding events3. These analyses look at this undesirable event and go backwards through the events that led to it, until the event which is considered the originator of the chain (the so called "root cause"), is identified. This is the case of methods such as Failure Mode and Effect Analysis (FMEA) or Failure Mode and Criticality Analysis (FMECA), also known as "Backward Looking" analyses. If instead an analysis is made to reveal all the possible chains of events in which something can go wrong, methods such as "Failure Tree Analysis" (FTA) are used. These are known as "Forward Looking" analysis methods.

Several other forward looking methods are also widely used, such as Hazard and Operability Analysis (HAZOP) and Event Tree Analysis (ETA).

All of these methods follow the "chain-of-failure-event" causality model, which can be best

represented through the analogy of a row of falling dominoes. There is an initial domino, labelled the "root cause", which represents a single event. It can be a human error, or a component failure. This error then propagates through the system, leading to other component failures and making eventually the last domino fall, where the problem is experienced.

This "family" of methods have been widely used since their invention in the 1950's. They are popular due to their relative simplicity, and effective in systems with technical components, as well as in simple systems involving both technical components and people, the so-called "socio-technical systems". A traditional way of quantifying cyber risks would be to identify all the ways a supply chain could fail (reliability analysis), or be subject to cyber-attack. This is best done in close interaction with an experienced team from different parts of the supply chain under analysis. The team will then agree on the likelihood of occurrence for each of these possible failures (Probability), and an approximate amount of money lost if these failures were to occur (Severity). Impact would then be Probability times Severity for each of these failures. By multiplying these two factors, a ranking of failures can be obtained, the events with highest impact can be identified, and actions can be concentrated on elimination or mitigation of these risks.

Our research at the Technical University is leading us to question several assumptions about how new risks such as cyber-risks can be managed, due to the increasing occurrence of different types of cyber-attacks with potentially harmful effects on supply chain performance. We have thus searched for other ways of understanding these risks, and that has lead us to specific, practical proposals to practitioners.

The traditional way of quantifying risks is faced with several shortcomings. We will analyze four of these4 : reliability versus safety, subjective choice, systemic effects, and dynamic behavior.

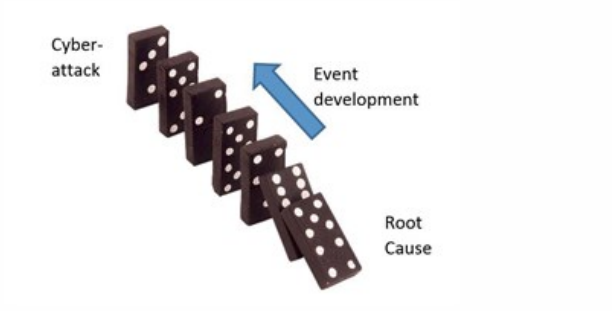

Figure 2 Representation of Chain-of -Failure as dominoes

Reliability versus safety

By focusing only on the performance of individual parts of the supply chain, there is the danger of confusing safety with reliability, meaning that it is generally assumed that if the components of the supply network function well, then the supply network is safe. This belief crumbles when errors occur in supply networks, where all components worked as expected, even sometimes BECAUSE all components worked as expected. This can happen particularly where some type of redundancy has been built into the system, or where controllers (human or automatic) do not understand adequately, what actually happens in the process. Redundancy can work well in simple mechanical or electrical systems, but when it is applied to decision networks, it can lead for example to a double call, where two different persons make contradicting decisions, a major problem in situations where urgent action is needed. Additionally, if the control actions in the procedures do not represent what should be done, then a correctly functioning control procedure could lead to an unwanted disruption.

Root cause depends on who does the analysis

In traditional risk assessment methods, there is a subjective choice of the chain of events. The list of potential failures, the chain of events leading to this failure, as well as the relationships between the events in the chain, right down to the "root cause", is highly dependent on who is doing the analysis. This can lead to several types of biases. If the participants are in management positions, without thorough knowledge of operations, then some relevant operational sources of accidents will be absent from the list. Root causes may be selected, just because they are politically acceptable, and other potential explanations will maybe not be explored, because they can be an embarrassment for the organization. Many times this search also ends with some type of "operator error" or "lack of training". Jens Rasmussen, a well-known researcher from Risø (present DTU) mentioned in the 1980's that it is indeed very difficult to analyze "through" a perceived human error, and therefore the analysis stops there.

Systemic effects: look at the wider picture

Only a very limited chain of events is taken into account in these traditional methods, and factors, not directly included in a chain of events, are excluded. The explanation usually considers the events that immediately lead to the loss, and systemic factors are not considered. Systemic factors can be the consequences the decision has in other parts of the organizaton, affecting and counteracting the original decision through feedback loops. This normally does not happen immediately. (See Figure 3). The systemic effects can also include policy decisions in the company, leading to the unwanted disruptions.
A proper understanding of the wanted behavior and the ability to withstand disruptions from cyber-attacks and regain normal operating conditions (cyber-resilience) is hidden in the traditional methods. The reaction by the company, when having to cope with a cyber-attack, will normally be a series of actions, using resources present in the company. These actions will develop over time, and the stability of the operation will eventually be restored. This will not happen immediately, and it will take some time. This means that cyber-resilience is in fact a dynamic behavior of the supply chain, and as such, it requires a way to deal with these dynamics. Let's look at this more closely.

Dynamics: Businesses versus cars

Dynamics can be better understood by comparing a manufacturing company subject to cyber-attacks, with a car on the road. A company manager would be equivalent to the car's driver. Cyber risks coming towards this company can be represented as obstacles on the road coming towards the car. The car has several controls that can be used by the driver to avoid these obstacles, such as the steering wheel, the accelerator, and the brakes to name a few. In the same way, the company has also some controls that can be used by the manager to "direct" the company development, such as setting strategic objectives, investment in training or incentive structures towards collaboration with suppliers, to name a few. The car has a mass that results in "inertial effects". It is not possible or convenient for the driver to change the car's direction suddenly, or accelerate or stop the car suddenly due to the risk of a crash. These inertial effects are also one of the characteristics for real systems, known as "dynamic effects". The company has also "inertial effects" such as the number of employees, the total accounts payable or the number of electronic orders for products. This means that a manager can't make sudden changes in the controls, in the case of risk of a cyber-attack, without other consequences.
A driver avoids an obstacle in the road by using the controls, for example by activating the brakes at a coming stop sign. A novice driver will maybe attempt to break too late, thrusting us forward with a jolt. A not-always-gentle reminder of the inertial effect of our own masses in movement. In the case of the company, a manager, attempting to avoid the effects of a cyber-attack, will use the controls at his disposal. A novice manager will maybe attempt to change strategic objectives too quickly or change the incentive structures radically, thereby creating an organizational "jolt".

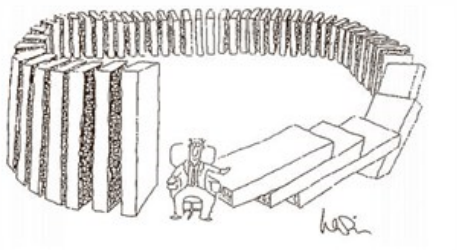

Figure 3 Dangers when feedback loops are not considered.

Many inertial effects are unknown to the manager

Some important differences come to light in this analogy, which we have defined as differences of "management" and differences of "design". Drivers normally start driving ("managing") the car from a resting position, and with training, the driver will gradually explore increasing levels of driving difficulty. In the case of the company, the manager will usually be appointed to the role, with the company already "in movement" at an undetermined speed. He will have a series of controls. Some of them will be familiar to him from his previous experience, and some might be new controls, implemented by his predecessor. There are different organizational "masses", which the manager will not necessarily know about, and he will have to discover by trial and error. Moreover, the manager will not have experience with the inertial effects, these controls at his disposal will have on the company. Finally, in the same way drivers are taught in the driving school about existing cars and driving conditions, managers are trained in business schools about existing companies and business conditions.
Another important and very relevant difference is one of design. The car has a structure, developed and improved over time by a team of specialists. They understand the effects this car structure has on the car's behavior, with special attention to dynamic effects. The structure of a company will usually not have been designed, but rather replicated initially from other working models, maybe grown through acquisition of other companies (inorganic

growth) or through its own expansion (organic growth). Company structures are therefore very likely to develop without any design considerations to its dynamics.

Control View of risks

Taking the car analogy further, resilience, or the ability to return to normal operations after disruptions, can be then understood as the ability of the company to adjust its course (its processes) by using its control structures. This can be represented in the following simplified figure 4. Resilience would then be reflected in how well this control structure works by:

- how well and timely do "sensors" measure the current process,
- how well and timely do we act on the process with our "actuators" when there is something to be done, and
- how well and timely can our supply chain translate what it is sensing into what it has to do about it, through its "controller".

This is an ongoing activity, since the supply process is constantly is encountering different working conditions that have to be detected and be adapted to.

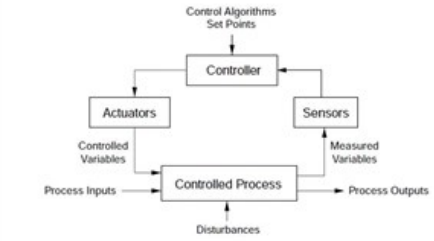

Figure 4 Control view of a process.

Steps to implement control view of cyber-resilience

Supply chain cyber resilience through the "control view" of cyber-risks can be achieved by the following general steps, accomplished by a team from the company under the guidance of experts in this type of analysis:

- Identify what the company will consider as undesirable disruptions to the supply chain (identify potential accidents)
- Identify the mix of conditions in the current supply network that would lead to the undesirable disruptions specified in the previous step (Identify hazards),
- Define the boundaries of what is in control and out of the control of the company (Identify supply system boundaries, controls and "masses" present in the system)
- Brainstorm about how each potential disruption, identified in the first step, could occur. This will lead to the identification of potential improved controls, which should be in place. For example, how the process is measured (sensors), organizational structures (actuators), or action plans for crisis management teams (controllers).

1Netlosses: Estimating the global cost of cybercrime, http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf
2Federal aviation administration. (2008). System safety handbook. Retrieved on September 24, 2015, from https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/

3These methods are based on the assumption that these events can be decomposed, that this decomposition allows for the independent analysis if each component, and that this does not influence the outcome. The process is known as "analytic reduction".
4Other shortcomings from the use of traditional risk assessment methods in supply networks, which we will not analyze in detail in this article, include aspects such as: a) their excessive search for guilt and operator error, instead of understanding the structure of the system that led to the disruption, b) assuming that two different events leading to a disruption will happen independently of each other, when analyzing how likely they are to happen, merely for mathematical simplicity, or c) The risk of "hindsight bias", this is, the perception of the disruption as foreseeable when looked after the fact, changing the discussion to "what was done wrong" instead of the more fruitful "why it made sense for the operators to make that decision at that time".